UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DAVID ANDREW, Individually and on behalf of all others similarly situated, Plaintiff, vs. LASTPASS US LP and GOTO TECHNOLOGIES USA, INC., Defendants.	Case No.: _____ **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiff David Andrew ("Andrew" or "Plaintiff") brings this complaint, by and through his attorneys and on behalf of all others similarly situated, against Defendant GoTo Technologies USA, Inc. ("GoTo") and its subsidiary LastPass US LP ("LastPass") (collectively "Defendants"), to seek redress for Defendants' actions preceding, surrounding, and following a data vulnerability and breach incident, which exposed the sensitive, personal information of millions of Defendants' customers. Plaintiff alleges as follows upon personal knowledge as to himself and his own experiences, and as to all other matters, upon information and belief, including an investigation and research conducted by his attorneys.

NATURE OF THE ACTION

1. Defendants failed to adequately protect the confidential and sensitive personal identifying information ("PII") of Plaintiff and other similarly situated LastPass users. This class action is brought on behalf of Class Members whose PII was stolen by online thieves in a cyber-attack (the "Data Breach") during which the cybercriminals accessed customers' PII by way of Defendants' password-protecting software system.

2. Defendants' failure to adequately implement and maintain data security practices and measures for stored PII directly and proximately caused injuries to Plaintiff and the Class.

3. Defendants failed to take adequate and reasonable steps to employ sufficient security measures or to properly protect sensitive PII, even in the face of well-publicized data breaches at numerous other businesses, financial institutions, and web platforms in previous years and months.

4. Despite numerous and highly publicized data breaches, Defendants failed to implement necessary and basic security measures to prevent the unauthorized access to this information, which was entrusted to Defendants for safekeeping by Plaintiff and the Class.

5. Defendants' customers nationwide have suffered real and imminent harm as a direct result of Defendants' conduct, including: (a) refusing to take adequate and reasonable measures to ensure its data systems, as well as the data stored therein, were protected from unauthorized third parties; (b) refusing to take appropriate steps to prevent the breach from occurring; (c) failing to disclose to and properly inform its customers of the material facts that it did not have adequate computer systems and security practices to safeguard PII; and (d) failing to provide timely and proper notice of the data breach to Plaintiff and the Class.

6. The Data Breach was the foreseeable and inevitable result of Defendants' inadequate data security measures and policies regarding data security. Despite well-known and highly publicized threats of security and data breaches, and despite the fact that data breaches were and are taking place across numerous industries, Defendants failed to ensure that they maintained adequate data security leaving the PII of Plaintiff and the Class subject to theft.

7. As a direct and proximate result of Defendants' negligence, an enormous amount of customer PII was taken from Defendant LastPass's storage system. Upon information and belief, Defendants' Data Breach compromised the PII of millions of—if not more—customers. Victims

of the Data Breach now have vulnerable PII, have had their privacy rights violated, have been exposed to increased risk of fraud and identity theft, have lost control over their personal and financial information, and have otherwise been injured.

8. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendants' inadequate conduct in the safeguarding of Class Members' PII that Defendants collected and improperly maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown third party.

9. Plaintiff, on behalf of himself and the Class, seeks (i) actual damages, economic damages, statutory damages, and/or nominal damages; (ii) punitive damages; (iii) injunctive relief; and (iv) fees and costs of litigation.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

11. This Court has personal jurisdiction over Defendants because Defendants' negligent acts or omissions, false and misleading misrepresentations, and violations of consumer protection statutes regarding the security of Plaintiff's and the Class's PII alleged herein occurred in this State. Defendants' principal places of business are also located in this State.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the injury in this case substantially occurred in this District and Defendants reside in this District.

PARTIES

13. Plaintiff David Andrew is, and was at all times relevant to this Complaint, a citizen of the State of Illinois. Andrew purchased his LastPass subscription on December 12, 2017, and he is still a subscribing member of LastPass. He received notice of the Data Breach from Defendant LastPass via email on December 1, 2022.

14. Defendant LastPass is a limited partnership organized under the laws of the State of Delaware with its principal place of business in Boston, Massachusetts.

15. Defendant GoTo is a corporation organized under the laws of the State of Delaware with its principal place of business in Massachusetts.

FACTUAL ALLEGATIONS

A. Defendant LastPass's Business

16. Defendant LastPass is a software company that provides services to businesses and consumers allowing them to store their passwords and other information in a secure location on the Internet.

17. Founded in 2008, LastPass describes itself as "leading the way in password security and identity management for personal and business digital safety."[1]

18. LastPass's About Us page continues, "Data breaches are on the rise, with more than 80% of breaches caused by weak, reused, or stolen passwords. Doing nothing could mean losing everything. That's why password security has never been more critical for individuals and business."[2]

[1] About LastPass, https//www.lastpass.com/company/about-us (last accessed Feb. 13, 2023).
[2] *Id*.

19. When consumers of LastPass create an account, they create what LastPass calls a "vault" of their passwords and sensitive data, including secure notes and credit card information.[3] LastPass instructs customers to think of their vault "like a physical safe but for your online valuables."[4] Although LastPass is a cloud-based security system, LastPass boasts the security of the program as unmatched because it employs "local-only encryption."[5]

20. LastPass states that data stored in customer's vaults is kept secret, even from LastPass itself, because the master password to the vault, and the codes used to encrypt and decrypt the secure data, are all stored in the user's device, and are never sent to LastPass's servers or accessible to LastPass.[6]

21. Once LastPass customers have set up their vault, LastPass records the websites with which customers hold accounts, as well as the login information for each of these sites and holds them in the vault. LastPass additionally retains the IP addresses that customers visit, showing the geolocation from which a user connects to the internet.

22. Further explaining their "foundation of security," LastPass's website also states, in regards to its "transparent incident response" that "Our team reacts swiftly to reports of bugs or vulnerabilities and communicates transparently with our community."[7]

B. LastPass Represented to Consumers That Its Service Was Private and Secure.

[3] How LastPass Works, https://www.lastpass.com/how-lastpass-works (last accessed Feb. 13, 2023).
[4] Password Vault Software, https://www.lastpass.com/features/password-vault (last accessed Feb. 13, 2023).
[5] *Id.*
[6] *Id.*
[7] A Foundation of Security, https://www.lastpass.com/security/zero-knowledge-security (last accessed Feb. 13, 2023).

23. Defendants boasted that their service was secure and claimed they would maintain the privacy and security of the PII of Plaintiff and the Class Members.

24. Defendant LastPass states that its service is designed to keep sensitive data safe using a "local-only, zero-knowledge security model."[8] LastPass describes the system as follows:

> The LastPass services features a vault, in which sensitive user data is stored and, based on utilization of a 'zero-knowledge' framework, accessed only by entering the user's master password, which is not maintained in unencrypted form by LastPass – LastPass does not store and cannot access this password. User data input via the LastPass web or mobile application is encrypted with the user's unique key on their device and the AES-256 encrypted data is synced to LastPass for secure storage. The user can access and decrypt their data on demand with their master password – which occurs entirely at the user and device-level.[9]

25. Under the Terms of Service for Personal Use, LastPass provides the following:

> "4.2 Your Privacy and Security
>
> 4.2.1. Information Security and Certifications
>
> **We have implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure**. We also maintain a compliance program that includes independent third-party audits and certifications. You can visit our Trust & Privacy Center (https://www.lastpass.com/trust-center) to review Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation), including, but not limited to, encryption use and standards, retention periods, and other helpful information.
>
> 4.2.2. Data Privacy
>
> **We maintain a global data privacy program, designed to safeguard and responsibly handle your Content and any associated personal data we may collect and/or process on your behalf**. You understand that when using the Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. You can visit our Trust &

[8] A Foundation of Security, https://www.lastpass.com/security/zero-knowledge-security (last accessed Feb. 13, 2023).
[9] *Id*.

> Privacy Center (https://www.lastpass.com/trust-center/privacy) to review LastPass' comprehensive privacy program, third-party frameworks, privacy policies, and applicable data processing locations and Sub-Processor Disclosures, as well as the TOMs."
>
> 8.7. Security Emergencies
>
> If we reasonably determine that the security of the Services or infrastructure may be compromised due to hacking attempts, denial of service attacks, or other malicious activities, we may temporarily suspend the Services. If we do so, we will, to the extent practicable, provide you notice, and take actions designed to promptly resolve any security issues and restore the Services.[10]

C. LastPass's Lax Security Practices Caused Customer Data to Be Breached.

26. Defendant GoTo is the parent company of LastPass and also stored the PII that was entrusted by Plaintiff and the Class to LastPass.

27. In August 2022, Defendants suffered a security breach that occurred on its storage systems.

28. LastPass initially issued a notice to customers on August 25, 2022 regarding the breach stating that unusual activity was detected on LastPass's servers several weeks earlier, but that no customer data was accessed during the activity. The letter stated that "we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults."[11] As it turned out, LastPass's initial assessment of the breach was incorrect, and customer information was, in fact, accessed by third parties.

[10] Terms of Service, https://www.lastpass.com/legal-center/terms-of-service/personal (last accessed Feb. 13, 2023) (emphasis added).
[11] Notice of Recent Security Incident, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/?sfdcid=7014P0000010Wn8QAE&gclid=CjwKCAiA3KefBhByEiwAi2LDHLsRzcsZx2b8EjqE4-07KpdoyiRQ1-NAn7uNCALVkUk8Hb2tI92CaxoCBKUQAvD_BwE (Last accessed Feb. 13, 2023).

29. In September 2022, LastPass issued another notice, again claiming that no customer data or PII was accessed, after performing a forensic investigation of the breach that occurred the month earlier. This notice stated, "Our investigation revealed that the threat actor's activity was limited to a four-day period in August 2022. During this time frame, the LastPass security team detected the threat actor's activity and then contained the incident. There is no evidence of any threat actor activity beyond the established timeline. We can also confirm that there is no evidence that this incident involved any access to customer data or encrypted password vaults."[12] Again, LastPass' statement regarding the breach was incomplete and inaccurate and provided customers with a false sense of security that their sensitive, personal information had not been accessed. The reality was much more serious.

30. On November 30, 2022, over three months after the breach occurred, Defendants issued a third notice finally acknowledging and admitting that the breach did in fact involve customer data. Defendants, however, continued to claim that no passwords could be accessed as a result of the breach. This notice stated, "We have determined that an unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information. Our customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture. . . . As always, we recommend that you follow our best practices around setup and configuration of LastPass, which can be found here. As part of our efforts, we continue to deploy enhanced security measures and monitoring capabilities across our infrastructure to help detect and prevent further threat actor activity."[13]

[12] *Id.*
[13] *Id.*

31. Finally, on December 22, 2022, LastPass issued a fourth notice to its customers admitting that along with customer data, customers' password vaults were taken in the cyberattack. In addition, LastPass acknowledged that substantial amounts of other customer information including payment information and other contact information was accessed in the breach. The notice stated the cybercriminals were "able to copy a backup of customer vault data from the encrypted storage container."[14] The notice continued, "While no customer data was accessed during the August 2022 incident, some source code and technical information were stolen from our development environment and used to target another employee, obtaining credentials and keys which were used to access and decrypt some storage volumes within the cloud-based storage service."[15]

32. In other words, although LastPass maintains that no customer data was accessed in August 2022, LastPass's failure to protect its technical systems during that initial breach—and its failure to adequately investigate and respond to the breach by protecting its core systems—resulted in further breaches between August and December 2022 that compromised its customers' data.

33. LastPass explained, "The threat actor was also able to copy a backup of customer vault data from the encrypted storage container which is stored in a proprietary binary format that contains both ***unencrypted data***, such as website URLs, as well as fully-encrypted sensitive fields such as website usernames and passwords, secure notes, and form-filled data."[16]

34. The hackers were able to access unencrypted customer vault data, which included "basic customer account information and related metadata including company names, end-user names,

[14] Lily Hay Newman, Yes, It's Time to Ditch LastPass, WIRED.com, (Dec. 28, 2022 2:35pm) (https://www.wired.com/story/lastpass-breach-vaults-password-managers/).
[15] *Supra* note 11.
[16] *Supra* note 11 (emphasis added).

billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service."[17]

35. In addition, although LastPass maintains that user passwords were encrypted, it nevertheless acknowledged that "[t]he threat actor may attempt to use brute force to guess your master password and decrypt the copies of vault data they took."[18] LastPass thus recommended that users "should consider minimizing risk by changing passwords of websites you have stored."[19]

36. Moreover, the way in which LastPass designed its password vaults "pose[s] a particular problem for users seeking to protect themselves in the wake of the breach, because changing that primary password now with LastPass won't do anything to protect the vault data that's already been stolen."[20]

37. As former LastPass security engineer Evan Johnson explained, "with vaults recovered, the people who hacked LastPass have unlimited time for offline attacks by guessing passwords and attempting to recover specific users' master keys."[21]

38. As a result of the Data Breach, Plaintiff and Class Members' sensitive PII, which was entrusted to Defendants to be securely stored, was compromised, unlawfully accessed, and stolen.

39. As a result of Defendants' conduct and/or inaction, Plaintiff and the Class Members were harmed and must now take burdensome and time-consuming remedial steps—including changing every password on every website they ever stored on LastPass—to protect themselves from future loss and harm. Indeed, Plaintiff and all Class Members are currently at a very high risk of misuse

[17] *See* Karim Toubba, Notice of Recent Security Incident, Update as of Thursday December 22, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last visited Jan. 18, 2023).
[18] *Supra* note 11.
[19] *Supra* note 11.
[20] *Supra* note 14.
[21] *Supra* note 14.

of their PII in the coming months and years, including but not limited to unauthorized account access on third-party services and identity theft through the use of PII to open new accounts.

40. Only in late December 2022, nearly half a year since the Data Breach, did LastPass begin notifying consumers of the full harmful extent of the Data Breach. The December notification also included instructions to customers to follow LastPass's "best practices" which included having a twelve-character minimum for master passwords, never reusing the same master password for a password on another website, and checking the number of iterations of the Password-Based Key Derivation Function ("PBKFD2"), the algorithm LastPass created for customers' master passwords. However, these steps may be too little, too late. If users had not already been following this complex security recommendation prior to the breach, any change now would not affect the password vault that are already in the hands of hackers.

41. Accordingly, Defendants acknowledged that they had lost control of information they stored from consumers who used their services.

42. On information and belief, even though millions of consumers have had their personal data breached due to Defendants' actions and inactions, Defendants have not specifically provided notice to all of these consumers.

D. LastPass's Customers' Data Is at Risk Because of the Data Breach.

43. As a result of Defendants' failure to properly and timely notify its customers of the full extent of the Data Breach, Class Members have not had an adequate opportunity to fully protect themselves and modify their passwords and other account credentials.

44. The cybercriminals were able to access Plaintiff's and the Class's PII because Defendants failed to take adequate measures to protect the PII they collected and stored. LastPass additionally failed to take adequate remedial actions by informing customers of their "best practices" and

therefore knowingly allowed customers to put their vaults at risk. Among other things, Defendants failed to implement data security measures designed to prevent this breach, despite multiple industry wide warnings regarding the risks of cyberattacks.

45. After the initial August 2022 breach occurred, Defendants failed to investigate the breach in a timely matter and failed to take adequate steps to prevent further intrusions as a result of the breach. Defendants' inaction resulted in their systems being further breached by hackers and caused the unnecessary and entirely preventable breach of their customers' data.

46. LastPass maintains that users who follow the best practices rule of LastPass to use a twelve-character or more master password will be safe from access to the passwords in their stolen vaults. However, users who signed up before 2018—when LastPass's best practices were implemented—never received notice of this change and can continue to login with their old passwords with fewer than twelve characters, without any prompt or requirements to update their password.

47. In addition, because LastPass was also storing users' IP addresses, hackers with access to vault information and the IP addresses used can create "movement profiles." Movement profiles are maps of a user's geographic locations using the IP addresses saved to their device (or LastPass vault). A movement profile can be created by unauthorized third parties with access to a user's IP addresses by using the addresses to map the geographic location of the Internet connection from the used device. Geolocating a user's IP address can provide a data thief with broad knowledge of a user's personal and private whereabouts on a daily basis, compromising their location data.[22]

[22] As an example of the data-privacy implications for the use of movement profiles and geolocation data, *see* Natasha Singer and Brian X. Chen, *In a Post-Roe World, the Future of Digital Privacy Looks Even Grimmer*, New York Times (Jul. 20, 2022) https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html. *See also* Sarah Emerson, *FTC Sues Geolocation Marketplace Over Abortion, Domestic Abuse Center Location Data*, Forbes (Aug. 29, 2022),

48. As a result of Defendants' failure to properly secure Plaintiff's and the Class's PII, Plaintiff and the Class's privacy has been violated. Consequently, Plaintiff's and the Class's PII is likely for sale to criminals on the dark web, and it is likely that additional unauthorized parties have accessed and viewed Plaintiff's and the Class's PII.

49. Following LastPass's December notice, a number of security experts spoke out against LastPass's handling of the data privacy and security failure and warned that it was downplaying the risks and harms from the Data Breach.

50. On December 26, 2022, security researcher Wladimir Palant published a blog post, "What's in a PR statement: LastPass breach explained."[23] In the post, Palant raised three critical concerns relative to (1) the mischaracterization of the Data Breach sequence of events, (2) the consequences of data breaches involving IP addresses, and (3) the heightened risk for certain users depending on their profile and the age of their account.

51. First, Palant explained that LastPass's attempt to separate the first August 2022 incident from the December 2022 Data Breach is a mischaracterization of the sequence of events:

> LastPass is trying to present the August 2022 incident and the data leak now as two separate events. But using information gained in the initial access in order to access more assets is actually a typical technique used by threat actors. It is called lateral movement.
>
> So the more correct interpretation of events is: we do not have a new breach now, **LastPass rather failed to contain the August 2022 breach. And because of that failure people's data is now gone.** Yes, this interpretation is far less favorable of LastPass, which is why they likely try to avoid it.[24]

---

https://www.forbes.com/sites/sarahemerson/2022/08/29/ftc-sues-geolocation-marketplace-over-abortion-domestic-abuse-center-location-data/?sh=2640d7461a35.

[23] *See* Wladimir Palant, What's in a PR statement: LastPass breach explained, Almost Secure (Dec. 26, 2022), https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/.

[24] *Id*. (emphasis added).

52. Palant also explained that LastPass's post-2019 requirement of a twelve-character minimum for master passwords, which they now tout as "best practices," was likely not utilized by many users. Accordingly, a large number of users are at heightened risk for further cyberattacks due to the LastPass Data Breach.

E. The LastPass Breach Exposed Users to the Risk of Identity Theft.

53. Identity theft, which costs Americans billions of dollars every year, occurs when an individual's PII is used without his or her consent to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, as well as hundreds if not thousands of dollars.

54. According to Javelin Strategy & Research, in 2018 alone over 16.7 million individuals were affected by identity theft, causing a loss of over $16.8 billion.

55. According to the Federal Trade Commission ("FTC"):

> Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

56. Consumers place a high value not only on their personal and financial information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" in addition to severe distress and other strong emotions and physical reactions.

57. The United States Government Accountability Office ("GAO") explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone

else's name."[25] The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

58. The FTC recommends that victims of identity theft take multiple steps to protect their personal and financial information following a data breach, including contacting one of the credit bureaus to place a fraud alert—such as an extended fraud alert that lasts for seven years and will inform consumers if someone steals their identity—reviewing their credit reports often, contacting companies to remove fraudulent charges from their accounts, placing a credit card freeze on their credit, and correcting their credit reports.

59. Identity thieves use stolen personal and financial information for "various types of criminal activities, such as when personal and financial [information] is used to commit fraud or other crimes," including "credit card fraud, phone or utilizes fraud, bank fraud and government fraud."[26]

60. The information obtained in the LastPass Data Breach can be used to commit identity theft by putting Plaintiff and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are ways for identity hackers to exploit information already in their possession to obtain more PII through fraudulent and unsolicited emails, text messages, and phone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

61. There is the possibility of a lapse in time between when the harm occurs to a victim of identity theft and when the harm is actually discovered, as well as a lapse between when the PII is stolen and when it is actually used. According to the U.S. GAO, which conducted a study regarding the growing number of data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[25] See In re Zappos.com, Inc., 888 F.3d 1020, 1024 (9th Cir. 2018).
[26] *Id*.

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

62. PII is such a valuable commodity to identity thieves that once the PII has been compromised, thieves often will trade the information on the "cyber black market" for months or even years.

63. Therefore, there is a strong likelihood that entire batches of stolen PII as a result of the LastPass Data Breach have been put on the cyber black market, or are waiting to be shared on the market, leaving Plaintiff and the Class members at an increased risk of fraud and identity theft for years to come.

64. Data breaches are not an unpreventable occurrence. In the DATA BREACH AND ENCRYPTION HANDBOOK, Lucy Thompson wrote, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She continued, "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."

65. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

66. Cyber criminals can use the PII to devise and implement phishing and social engineering schemes capitalizing on the authentic information stolen from Defendants' systems to send fraudulent mail, emails, and other communications to Plaintiff and Class members that look

[27] *See* GAO Report, at p.29.

authentic, but in fact are designed to persuade them into paying money or providing additional sensitive information that can then be used to steal funds.

67. Cyber criminals can use the financial information that Defendants were entrusted to safeguard to perpetrate financial crimes that harm Plaintiff and the Class, or as what appears to have happened to Defendants in this instance, cyber criminals can leverage pieces of information to gain access to additional information that they can then use to carry out significant financial harm to victims. In addition to all the other immediate consequences of the LastPass Data Breach, Plaintiff and Class Members face a substantially increased risk of identity theft.

PLAINTIFF'S INJURIES

68. On December 12, 2017, Plaintiff David Andrew saw the representations from Defendants claiming they had superior data security. Those representations were false, deceptive, and misleading. Andrew reasonably relied on these misrepresentations and, on December 12, 2017, purchased a subscription to LastPass.

69. On December 1, 2022, for the first time, Andrew received an email from LastPass informing him of a "security incident" on a third-party cloud storage service during which an unauthorized party gained access to elements of customer information. The notice claimed that LastPass was steadfast in their confidence that customer passwords remained safe due to their Zero Knowledge architecture, but that users should be sure to maintain "best practices."

70. If Andrew had known the true risks associated with using Defendants' LastPass service, including its deficient and unreasonable data security practices, he would not have subscribed to LastPass. Because Andrew reasonably relied on Defendants' misrepresentations, he suffered damages in the amount of money paid for services and quality bargained for but not received.

71. Moreover, following the Data Breach, Andrew dedicated time, energy, and resources researching the Data Breach, investigating the facts and circumstances, conducting his own risk assessment, and changing all of his passwords for the accounts using LastPass—roughly 500 passwords that he had stored in LastPass. In the months since disclosure of the Data Breach, Andrew has dedicated hours of his life to attempting to remedy the harm and prevent future harm caused by the breach by sorting through line by line the passwords he entrusted to Defendants.

72. As of the date this complaint is filed, Andrew has still not completed the mitigation of the Data Breach, due to the extensive PII he had stored in Defendants' systems. He was diverted from performing money-making services such as working while attempting to remedy the potential harm caused by Defendants' Data Breach.

CLASS ALLEGATIONS

73. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and the Class defined as follows:

All persons who had their Customer Information accessed in the Data Breach.

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interests and its current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

74. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but individual joinder is impracticable. LastPass claims a user base of over thirty-three million people and over 100,000 business clients.[28]

75. **Typicality**: Plaintiff's claims are typical of the claims of other members of the Class, in that Plaintiff and Class members sustained damages arising out of the same action or inaction of Defendants relating to their failure to adequately protect, oversee, monitor, and safeguard the Customer Information.

76. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiff's claims are made in a representative capacity on behalf of the other members of the Class. Plaintiff has no interests antagonistic to the interests of the other members of the Class and is subject to no unique defenses. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so.

77. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' practices challenged herein apply to and affect all Class members uniformly, and Plaintiff's challenge to those practices hinge on

[28] About Us, LastPass, https://www.lastpass.com/company/about-us (last accessed Feb. 10, 2023).

Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

78. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, not are not necessarily limited to the following:

a. Whether Defendants failed to maintain adequate security procedures;

b. Whether Defendants' conduct constitutes negligence;

c. Whether Defendants' conduct constitutes negligent misrepresentation;

d. Whether Defendants' conduct constitutes a breach of contract;

e. Whether Plaintiff and Class members are entitled to restitution on the basis of unjust enrichment; and

f. Whether Plaintiff and Class members are entitled to damages and injunctive relief.

79. **Superiority**: This case is appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. Joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small in comparison to the burden and expense of individual prosecutions of litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties and the court systems of many states and federal districts. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication,

economy of sale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

CAUSES OF ACTION

COUNT I
Negligence

80. Plaintiff incorporates paragraphs 1-54 as if fully set forth herein.

81. Each Defendant owed a duty to Plaintiff and Class members to properly notify them that their Customer Information had been disclosed to and accessed by unauthorized third-party cyber criminals.

82. Each Defendant owed a duty to Plaintiff and the Class to properly train, vet, and oversee employees and vendors who maintain, access, store, and manage Plaintiff's and Class members' PII and to implement and maintain reasonable data security practices to protect the Customer Information from foreseeable cyberattacks and unauthorized access.

83. Defendants breached these duties and the applicable standards of care by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) storing Plaintiff's and the Class's PI;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the cybercriminals' infiltration into the system(s) storing Plaintiff's and the Class's PII;

d. Failing to adequately separate and isolate PII from publicly accessible or publicly adjacent environments in their systems;

e. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the Class's PII;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiff's and the Class's PII reasonably and appropriately in order to prevent or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII to ensure the PII was being stored and maintained for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and the Class's PII;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiff's and the Class's PII was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the Class members regarding the circumstances and extent of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding the disposition of Plaintiff's and Class members' PII at all times during the Data Breach.

84. Defendants are both the actual and legal cause of Plaintiff's and the Class members' harms and injuries. Had Defendants implemented and maintained adequate data security measures and provided timely notification of the Data Breach to affected consumers, including Plaintiff and Class members, Plaintiff and Class members would not have been damaged or would have been damaged to a lesser degree than they actually were.

85. Plaintiff and the Class members have suffered damages as a result of Defendants' negligence. Plaintiff and Class members have suffered actual and concrete injuries and will continue to suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendants' warnings and following their instructions in the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of the benefit of the bargained for data security practices that were not provided as represented; and (i) and diminution of value of their PII.

COUNT II
Negligent Misrepresentation

86. Plaintiff incorporates paragraphs 1- 54 as if fully set forth herein.

87. Defendants supplied false information for the guidance of others in the course of their business. As alleged in the preceding paragraphs, Defendants falsely represented that their products and services were superior data security practices that would protect Plaintiff and the Class from the Data Breach, when in reality, Defendants maintained deficient and unreasonable data security practices.

88. Defendants' representations were false, and Defendants failed to exercise reasonable care in obtaining or communicating the information. Defendants' data security measures were unreasonable and deficient by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and the Class's PII;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the Class's PII;

d. Failing to adequately separate and isolate PII from publicly accessible or publicly adjacent environments;

e. Failing to implement and maintain adequate safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the Class members' PII;

f. Failing to monitor and detect their confidential and sensitive data environments(s) storing Plaintiff's and the Class members' PII reasonably and appropriately in order to prevent or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention policies and procedures with respect to the PII to ensure PII was being stored and maintained only for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and the Class members' PII;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiff's and the Class members' PII was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Brach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notice to Plaintiff and the Class regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding

the disposition of Plaintiff's and the Class members' PII at all times during the Data Breach.

89. Plaintiff and the Class reasonably relied on Defendants' false information and were justifiably induced to obtain Defendants' products and services in reliance thereon.

90. Plaintiff and the Class have suffered damages as a result of Defendants' negligent misrepresentations. Plaintiff and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendants' warnings and following their instructions in the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of the benefit of the bargained for data security practices that were not provided as represented; and (i) diminution of value of their PII.

COUNT III
Breach of Contract

91. Plaintiff incorporates paragraphs 1-54 as if fully set forth herein.

92. Defendant LastPass promises in its Personal Terms of Service:

> 4.2.1. Information Security and Certifications
> We have implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure. We also maintain a compliance program that includes independent third-party audits and certifications. You can visit out Trust & Privacy Center (http://www.lastpass.com/trust-center) to review Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation), including, but not limited to, encryption use and standards, retention periods, and other helpful information.

> 4.2.2. Data Privacy
> We maintain a global data privacy program, designed to safeguard and responsibly handle your Content and any associated personal data we may collect and/or process on your behalf. You understand that when using the Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. You can visit our Trust & Privacy Center (http://www.lastpass.com/trust-center/privacy) to review LastPass' comprehensive privacy program, third-party frameworks, privacy policies, and applicable data processing locations and Sub-Processor Disclosures, as well as the TOMs.

93. Defendant LastPass promises in its Business Terms of Service:

> 4.2.1. Information Security and Certifications
> LastPass agrees to maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure, in accordance with industry standards. Additional information about LastPass' technical and organizational security measures ("TOMs"), including, but not limited to, encryption use and standards, retention periods, and other helpful information can be found in our Trust & Privacy Center (http://www.lastpass.com/trust-center), along with information regarding our independent third-party security audits and certifications.
>
> 4.2.2. Data Privacy
> While providing the Services to you, LastPass agrees to handle your Content and any associated personal data we may collect and/or process on your behalf in a responsible manner. You can visit our Trust & Privacy Center (http://www.lastpass.com/trust-center/privacy) to review additional information about LastPass' comprehensive privacy program, third-party privacy frameworks, privacy policies, and applicable data processing locations and Sub-Processor Disclosures. You understand that when using our Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. When providing our Services, LastPass acts as a data processor, service provider, or the equivalent construct. To review and execute LastPass' Data Processing Addendum ("DPA"), please visit https://www.lastpass.com/legal-center.[29]

94. Defendant GoTo promises in its Terms of Service:

> 4.2. Your Privacy and Security.
> We maintain a global privacy and security program designed to protect your Content and any associated personal data we may collect and/or process on your behalf. You can visit our Trust & Privacy Center (http://www.goto.com/company/trust) to review applicable data processing

[29] https://www.lastpass.com/legal-center/terms-of-service/business (last accessed Feb. 10, 2023).

> locations and Sub-Processor Disclosures, as well as Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation). When providing our Services, we act as a data processor, service provider, or the equivalent construct. To review and execute our Data Processing Addendum ("DPA"), please visit https://www.goto.com/company/legal.[30]

95. Additionally, Defendant GoTo incorporates its security measure representations into its Terms of Service, as follows:

> GoTo is dedicated to monitoring and continuously improving our security, technical and organizational measures to better protect your sensitive Customer Content. We are always evaluating industry standard practices regarding technical data privacy and information security and strive to meet or exceed those standards. Our security programs are comprehensive and dedicated to all facets of security.
>
> Alongside our stringent internal security controls, we hold the following trusted third-party security certifications. As part of our commitment to our subscribers, we conduct SOC 2 (type II) audits, and share out a SOC 3 report, which is a shareable version of the SOC 2. The SOC 3 reports for each applicable product, can be found and downloaded on our product resources page here.[31]

96. Defendants breached the foregoing contractual terms resulting in the Data Breach, in one or more of the following ways:

    a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

    b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and Class members' PII;

    c. Failing to maintain adequate and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were

[30] https://www.goto.com/company/legal (last accessed Feb. 10, 2023).
[31] https://www.goto.com/company/trust/security-measures (last accessed Feb. 10, 2023).

the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the Class members' PII;

d. Failing to adequately separate and isolate PII from publicly accessible or publicly adjacent environment(s);

e. Failing to implement and maintain adequate safeguards and procedures to prevent the unauthorized access to Plaintiff's and Class members' PII;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiff's and Class members' PII reasonably and appropriately in order to prevent or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII to ensure the PII was being stored and maintained only for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and Class members' PII;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiff's and Class members' PII, was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data

Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding the disposition of Plaintiff's and Class members' PII at all times during the Data Breach.

97. All conditions precedent were performed or have occurred.

98. As a proximate result of Defendants' breaches of contract described above, Plaintiff and Class members have incurred damages. Plaintiff and Class members have suffered actual an concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendants' warnings and following their instructions in the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of the benefit of the bargained for data security practices that were not provided as represented; and (i) diminution of value of their PII.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of the Class, requests that the Court:

A. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned counsel as Class counsel;

B. Award equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Award damages to Plaintiff and the Class in an amount to be determined at trial;

D. Award Plaintiff and Class members their reasonable litigation expenses and attorneys' fees to the extend allowed by law;

E. Award Plaintiff and Class member pre- and post-judgment interest, to the extent allowable; and

F. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

By: */s/ Patrick J. Vallely*

Edward F. Haber (BBO# 215620)
Patrick J. Vallely (BBO# 663866)
Nicole E. Dill (BBO# 709113)
SHAPIRO HABER & URMY LLP
One Boston Place, Suite 2600
Boston, MA 02108
Telephone: (617) 439-3939
Facsimile: (617) 439-0134
ehaber@shulaw.com
pvallely@shulaw.com
ndill@shulaw.com

Robert C. Schubert (*pro hac vice* to be filed)
Amber L. Schubert (*pro hac vice* to be filed)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

Attorneys for Plaintiff Andrew and the Putative Class